Theoretical Computer Science
Algorithms, automata, complexity and games

Volume 226, Numbers 1–2, 17 September 1999

Cryptography

Guest Editor: C. Ding

Abstracted/Indexed in: ACM Computing Reviews, Compuscience, Computer Abstracts, Current Contents: Engineering, Technology & Applied Science, Engineering Index/Compendex, INSPEC Information Services, Mathematical Reviews, Zentralblatt für Mathematik

Contents

Preface

C. Ding 1

Biography

J. Karhumäki
A short biography of Arto Salomaa 3

Contributions

L.M. Adleman, J. DeMarrais and M.-D. Huang
A subexponential algorithm for discrete logarithms over hyperelliptic curves of large genus over GF(q) 7

S.K. Chua, K.H. Leung and S. Ling
Attack on RSA-type cryptosystems based on singular cubic curves over Z/nZ 19

T.W. Cusick
The Ajtai random class of lattices 29

D. Feng
Three characterizations of correlation-immune functions over rings Z_N 37

D. Gollmann
Dual bases and bit-serial multiplication in $\mathbf{F}_{q^n}$ 45

A. Klapper and J. Xu
Algebraic feedback shift registers 61

H. Niederreiter and M. Vielhaber
An algorithm for shifted continued fraction expansions in parallel linear time 93

V. Niemi and A. Renvall
Efficient voting with no selling of votes 105

Theoretical Computer Science
Algorithms, automata, complexity and games

Volume 226, Numbers 1–2, 17 September 1999

Cryptography

Guest Editor: C. Ding

Abstracted/Indexed in: ACM Computing Reviews, Compuscience, Computer Abstracts, Current Contents: Engineering, Technology & Applied Science, Engineering Index/Compendex, INSPEC Information Services, Mathematical Reviews, Zentralblatt für Mathematik

Contents

Preface

C. Ding 1

Biography

J. Karhumäki
A short biography of Arto Salomaa 3

Contributions

L.M. Adleman, J. DeMarrais and M.-D. Huang
A subexponential algorithm for discrete logarithms over hyperelliptic curves of large genus over GF(q) 7

S.K. Chua, K.H. Leung and S. Ling
Attack on RSA-type cryptosystems based on singular cubic curves over Z/nZ 19

T.W. Cusick
The Ajtai random class of lattices 29

D. Feng
Three characterizations of correlation-immune functions over rings Z_N 37

D. Gollmann
Dual bases and bit-serial multiplication in $\mathbf{F}_{q^n}$ 45

A. Klapper and J. Xu
Algebraic feedback shift registers 61

H. Niederreiter and M. Vielhaber
An algorithm for shifted continued fraction expansions in parallel linear time 93

V. Niemi and A. Renvall
Efficient voting with no selling of votes 105

J. Ó Ruanaidh, H. Petersen, A. Herrigel, S. Pereira and T. Pun
Cryptographic copyright protection for digital images based on watermarking techniques 117

R. Tao and S. Chen
On finite automaton public-key cryptosystem 143

V. Varadharajan, K.Q. Nguyen and Y. Mu
On the design of efficient RSA-based off-line electronic cash schemes 173

C. Zhang, K.-Y. Lam and S. Jajodia
Scalable threshold closure 185

Y. Zheng, X.-M. Zhang and H. Imai
Restriction, terms and nonlinearity of Boolean functions 207

Author index volume 226 225